Interference & updated Search 09/783,049

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	("password$1.clm. andauthentication.clm.anddevice. clm.andaccess.clm.anduser.clm. andmemory.clm.and"timeinterval". clm.and"userdevice".clm. and"authenticationdevice".clm. andcharachteristics.clm.").PN.	USPAT	OR	OFF	2006/02/23 20:05
L2	0	password$1.clm. and authentication.clm. and "device. clm.and" access.clm. and user. clm. and memory.clm. and "time interval".clm. and "user device". clm. and "authentication device". clm. and charachteristics.clm.	USPAT	OR	OFF	2006/02/23 20:07
L3	0	password$1.clm. and authentication.clm. and "device. clm.and" access.clm. and user. clm. and memory.clm. and "time interval".clm. and "user device". clm. and "authentication device". clm.	USPAT	OR	OFF	2006/02/23 20:08
L4	168	password$1.clm. and authentication.clm. and "device. clm.and" access.clm. and user. clm. and memory.clm. and "time interval".clm.	USPAT	OR	OFF	2006/02/23 20:07
L5	5	4 and "user device"	USPAT	OR	OFF	2006/02/23 20:07
L6	0	5 and "authentication device"	USPAT	OR	OFF	2006/02/23 20:07
L7	1	password$1.clm. and authentication.clm. and "device. clm.and" access.clm. and user. clm. and memory.clm. and "time interval".clm. and "user device". clm. and "authentication device". clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/23 20:08
L8	309	password$1.clm. and authentication.clm. and "device. clm.and" access.clm. and user. clm. and memory.clm. and "time interval".clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/23 20:11
L9	269	713/184	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/23 20:09

EAST Search History

L10	7660	713/184 or 713/183 or 713/170 or 713/201 or 726/28 or 726/29	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/23 20:09
L11	7660	10 or 9	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/23 20:09
L12	11	11 and 8	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/23 20:09
L13	2035	pritchard.inv.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/23 20:10
L14	198	pritchard.inv. and james	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/23 20:10
L15	7	password$1 and authentication and device and access and user and memory and "time interval" and "user device" and "authentication device"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/23 20:20
L16	0	password$1 and authentication and device and access and user and memory and "time interval" and "user device" and "14 and 15authentication device"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/23 20:13
L17	1	14 and 15	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/23 20:13

EAST Search History

L18	164	705/72	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/23 20:20
L19	51	18 and 11	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/23 20:21

Terms used
characher$6 and **password$1** and **authentication** and **device** and **access** and **user** and **memory** and **time interval** and **user device** and **authentication device**

Fc
17,
171,

Sort results by relevance

Display results expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 SPINS: security protocols for sensor networks

Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler
September 2002 **Wireless Networks**, Volume 8 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(213.37 KB) Additional Information: full citation, abstract, references, citings, index terms

Wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. We present a suite of security protocols optimized for sensor networks: SPINS. SPINS has two secure building blocks: SNEP and µTESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. µTESLA provides authenticated broadcast for severely resource-constrained ...

Keywords: MANET, authentication of wireless communication, cryptography, mobile ad hoc networks, secrecy and confidentiality, secure communication protocols, sensor networks

2 Applications on the go: MediaAlert: a broadcast video monitoring and alerting system for mobile users

Bin Wei, Bernard Renger, Yih-Farn Chen, Rittwik Jana, Huale Huang, Lee Begeja, David Gibbon, Zhu Liu, Behzad Shahraray
June 2005 **Proceedings of the 3rd international conference on Mobile systems, applications, and services MobiSys '05**

Publisher: ACM Press

Full text available: pdf(593.10 KB) Additional Information: full citation, abstract, references

We present a system for automatic monitoring and timely dissemination of multimedia information to a range or mobile information appliances based on each user's interest profile. Multimedia processing algorithms detect and isolate relevant video segments from over twenty television broadcast programs based on a collection or words and phrases specified by the user. Content repurposing techniques are then used to convert the information into a form that is suitable for delivery to the user's mobi ...

Keywords: alerting, automatic speech recognition (ASR), content adaptation, content repurposing, mobile devices, multimedia messaging, multimedia processing, news monitoring, notification, service platform

3 SPINS: security protocols for sensor netowrks

Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar

July 2001 **Proceedings of the 7th annual international conference on Mobile computing and networking**

Publisher: ACM Press

Full text available: pdf(242.17 KB) Additional Information: full citation, abstract, references, citings, index terms

As sensor networks edge closer towards wide-spread deployment, security issues become a central concern. So far, much research has focused on making sensor networks feasible and useful, and has not concentrated on security.

We present a suite of security building blocks optimized for resource-constrained environments and wireless communication. SPINS has two secure building blocks: SNEP and &mgr;TESLA SNEP provides the following important baseline security primitives: Data confidentia ...

4 Deployment and testbeds: Enhancement of a WLAN-based internet service in Korea

Youngkyu Choi, Jeongyeup Paek, Sunghyun Choi, Go Woon Lee, Jae Hwan Lee, Hanwook Jung

September 2003 **Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots**

Publisher: ACM Press

Full text available: pdf(774.23 KB) Additional Information: full citation, abstract, references, index terms

A wireless LAN (WLAN)-based Internet service, called NESPOT, of Korea Telecom (KT), the biggest telecommunication and Internet service company in Korea, has been operational since early 2002. As the numbers of subscribers and deployed access points (APs) increase, KT has been endeavoring to improve its service quality as well as the network management. In this paper, we introduce a joint effort between Seoul National University (SNU) and KT to achieve it. We have been addressing two major issues ...

Keywords: IEEE 802.11, LAN, hotspot service, wireless internet service provider (WISP)

5 The Cricket location-support system

Nissanka B. Priyantha, Anit Chakraborty, Hari Balakrishnan

August 2000 **Proceedings of the 6th annual international conference on Mobile computing and networking**

Publisher: ACM Press

Full text available: pdf(1.22 MB) Additional Information: full citation, abstract, references, citings

This paper presents the design, implementation, and evaluation of Cricket, a location-support system for in-building, mobile, location-dependent applications. It allows applications running on mobile and static nodes to learn their physical location by using listeners that hear and analyze information from beacons spread throughout the building. Cricket is the result of several design goals, including user privacy, decentralized administrat ...

6 Distributed PIN verification scheme for improving security of mobile devices

Jian Tang, Vagan Terziyan, Jari Veijalainen

April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2

Publisher: Kluwer Academic Publishers

Full text available: pdf(298.43 KB) Additional Information: full citation, abstract, references, index terms

The main driving force for the rapid acceptance rate of small sized mobile devices is the capability to perform e-commerce transactions at any time and at any place, especially while on the move. There are, however, also weaknesses of this type of e-commerce, often called mobile e-commerce, or m-commerce. Due to their small size and easy portability mobile devices can easily be lost or stolen. Whereas the economic values and privacy threats

protected with Personal Identification Numbers (PIN) ar ...

Keywords: measure, mobile device, probability, risks, security, uncover

7 Detecting past and present intrusions through vulnerability-specific predicates

Ashlesha Joshi, Samuel T. King, George W. Dunlap, Peter M. Chen

October 2005 **ACM SIGOPS Operating Systems Review , Proceedings of the twentieth ACM symposium on Operating systems principles SOSP '05**, Volume 39 Issue 5

Publisher: ACM Press

Full text available: pdf(261.66 KB) Additional Information: full citation, abstract, references, index terms

Most systems contain software with yet-to-be-discovered security vulnerabilities. When a vulnerability is disclosed, administrators face the grim reality that they have been running software which was open to attack. Sites that value availability may be forced to continue running this vulnerable software until the accompanying patch has been tested. Our goal is to improve security by detecting intrusions that occurred before the vulnerability was disclosed and by detecting and responding to intr ...

Keywords: IntroVirt, intrusion detection, semantic gap, virtual-machine introspection, virtual-machine replay, vulnerability-specific predicates

8 Ubiquitous computing/security: Towards a new paradigm for securing wireless sensor networks

K. Jones, A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy

August 2003 **Proceedings of the 2003 workshop on New security paradigms**

Publisher: ACM Press

Full text available: pdf(718.31 KB) Additional Information: full citation, abstract, references, citings

The network model assumed in this paper consists of tiny, energy-constrained, commodity sensors massively deployed alongside with one or more sink nodes that provide the interface to the outside world. The sensors in the network are initially anonymous and unaware of their location. Our main contribution is to propose a new robust and energy-efficient solution for secure operation of wireless sensor networks. The paper motivates a new paradigm where security is based upon using parameterized fre ...

Keywords: energy-efficient protocols, frequency hopping, security, wireless sensor networks

9 Access control to people location information

Urs Hengartner, Peter Steenkiste

November 2005 **ACM Transactions on Information and System Security (TISSEC)**, Volume 8 Issue 4

Publisher: ACM Press

Full text available: pdf(356.85 KB) Additional Information: full citation, abstract, references, index terms

Ubiquitous computing uses a variety of information for which access needs to be controlled. For instance, a person's current location is a sensitive piece of information that only authorized entities should be able to learn. Several challenges arise in the specification and implementation of policies controlling access to location information. For example, there can be multiple sources of location information. The sources can be within different administrative domains, which might allow differen ...

Keywords: Certificates, DSA, RSA, SPKI/SDSI, credential discovery, delegation, location, privacy, trust

10 Personal trusted devices for web services: revisiting multilevel security
Edgar Weippl, Wolfgang Essmayr
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2
Publisher: Kluwer Academic Publishers
Full text available: pdf(109.95 KB) Additional Information: full citation, abstract, references, index terms

In this paper we revisit the concept of mandatory access control and investigate its potential with personal digital assistants (PDA). Only if applications are clearly separated and Trojans cannot leak personal information can these PDAs become personal trusted devices. Limited processing power and memory can be overcome by using Web services instead of full-fledged applications - a trend also in non-mobile computing. Web services, however, introduce additional security risks, some of them speci ...

Keywords: multilevel security (MLS), personal digital assistant (PDA), personal trusted device (PTD), trusted computing base (TCB)

11 Next generation access control models: Implementing access control to people location information
Urs Hengartner, Peter Steenkiste
June 2004 **Proceedings of the ninth ACM symposium on Access control models and technologies**
Publisher: ACM Press
Full text available: pdf(164.30 KB) Additional Information: full citation, abstract, references, index terms

Ubiquitous computing uses a variety of information for which access needs to be controlled. For instance, a person's current location is asensitive piece of information, which only authorized entities should be able to learn. Several challenges arise in the specification and implementation of policies controlling access to location information. For example, there can be multiple sources of location information, the sources can be within different administrative domains, different administrative ...

Keywords: certificates, delegation, dsa, location, rsa, spki/sdsi, trust

12 Context awareness: A context-aware group management middleware to support resource sharing in MANET environments
Dario Bottazzi, Antonio Corradi, Rebecca Montanari
May 2005 **Proceedings of the 6th international conference on Mobile data management MEM '05**
Publisher: ACM Press
Full text available: pdf(1.00 MB) Additional Information: full citation, abstract, references

Recent advances in Mobile Ad-hoc NETworks (MANET) technologies promote new opportunities for users to share resources from ubiquitous points of attachment, when changing physical locations and even when no statically deployed network infrastructure is available. However, the highly dynamic nature of Mobile Ad-Hoc environments causes users to experience continuous changes in the set of the locally accessible resources, thus increasing the complexity of resource sharing. Novel middleware solutions ...

13 Improving the browsing experience: WebPod: persistent Web browsing sessions with pocketable storage devices
Shaya Potter, Jason Nieh
May 2005 **Proceedings of the 14th international conference on World Wide Web**
Publisher: ACM Press

Full text available: pdf(166.59 KB) Additional Information: full citation, abstract, references, index terms

We present WebPod, a portable system that enables mobile users to use the same persistent, personalized web browsing session on any Internet-enabled device. No matter what computer is being used, WebPod provides a consistent browsing session, maintaining all of a user's plugins, bookmarks, browser web content, open browser windows, and browser configuration options and preferences. This is achieved by leveraging rapid improvements in capacity, cost, and size of portable storage devices. WebPod p ...

Keywords: checkpoint/restart, portable storage, process migration, virtualization, web browsing

14 A secure infrastructure for service discovery and access in pervasive computing
Jeffrey Undercoffer, Filip Perich, Andrej Cedilnik, Lalana Kagal, Anupam Joshi
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2
Publisher: Kluwer Academic Publishers
Full text available: pdf(308.34 KB) Additional Information: full citation, abstract, references, citings, index terms

Security is paramount to the success of pervasive computing environments. The system presented in this paper provides a communications and security infrastructure that goes far in advancing the goal of anywhere-anytime computing. Our work securely enables clients to access and utilize services in heterogeneous networks. We provide a service registration and discovery mechanism implemented through a hierarchy of service management. The system is built upon a simplified Public Key Infrastructure t ...

Keywords: distributed services, extensible markup language, pervasive computing, security, smartcards

15 Papers from MC^{2}R open call: Access and mobility of wireless PDA users
Marvin McNett, Geoffrey M. Voelker
April 2005 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 9 Issue 2
Publisher: ACM Press
Full text available: pdf(595.52 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we analyze the mobility patterns of users of wireless hand-held PDAs in a campus wireless network using an eleven week trace of wireless network activity. Our study has two goals. First, we characterize the high-level mobility and access patterns of hand-held PDA users and compare these characteristics to previous workload mobility studies focused on laptop users. Second, we develop two wireless network topology models for use in wireless mobility studies: an *evolutionary topol* ...

16 Fast detection of communication patterns in distributed executions
Thomas Kunz, Michiel F. H. Seuren
November 1997 **Proceedings of the 1997 conference of the Centre for Advanced Studies on Collaborative research**
Publisher: IBM Press
Full text available: pdf(4.21 MB) Additional Information: full citation, abstract, references, index terms

Understanding distributed applications is a tedious and difficult task. Visualizations based on process-time diagrams are often used to obtain a better understanding of the execution of the application. The visualization tool we use is Poet, an event tracer developed at the University of Waterloo. However, these diagrams are often very complex and do not provide the user with the desired overview of the application. In our experience, such tools display repeated occurrences of non-trivial commun ...

17 DMSEC session: User re-authentication via mouse movements

Maja Pusara, Carla E. Brodley

October 2004 **Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security**

Publisher: ACM Press

Full text available: pdf(179.25 KB) Additional Information: full citation, abstract, references, index terms

We present an approach to user re-authentication based on the data collected from the computer's mouse device. Our underlying hypothesis is that one can successfully model user behavior on the basis of user-invoked mouse movements. Our implemented system raises an alarm when the current behavior of user X, deviates sufficiently from learned "normal" behavior of user X. We apply a supervised learning method to discriminate among k users. Our empirical results for eleven users show that we can ...

Keywords: anomaly detection, mouse dynamics, user re-authentication

18 System support for pervasive applications

Robert Grimm, Janet Davis, Eric Lemar, Adam Macbeth, Steven Swanson, Thomas Anderson, Brian Bershad, Gaetano Borriello, Steven Gribble, David Wetherall

November 2004 **ACM Transactions on Computer Systems (TOCS)**, Volume 22 Issue 4

Publisher: ACM Press

Full text available: pdf(1.82 MB) Additional Information: full citation, abstract, references, index terms

Pervasive computing provides an attractive vision for the future of computing. Computational power will be available everywhere. Mobile and stationary devices will dynamically connect and coordinate to seamlessly help people in accomplishing their tasks. For this vision to become a reality, developers must build applications that constantly adapt to a highly dynamic computing environment. To make the developers' task feasible, we present a system architecture for pervasive computing, called & ...

Keywords: Asynchronous events, checkpointing, discovery, logic/operation pattern, migration, one.world, pervasive computing, structured I/O, tuples, ubiquitous computing

19 Distributed operating systems

Andrew S. Tanenbaum, Robbert Van Renesse

December 1985 **ACM Computing Surveys (CSUR)**, Volume 17 Issue 4

Publisher: ACM Press

Full text available: pdf(5.49 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Distributed operating systems have many aspects in common with centralized ones, but they also differ in certain ways. This paper is intended as an introduction to distributed operating systems, and especially to current university research about them. After a discussion of what constitutes a distributed operating system and how it is distinguished from a computer network, various key design issues are discussed. Then several examples of current research projects are examined in some detail ...

20 Making computers disappear: appliance data services

Andrew C. Huang, Benjamin C. Ling, John Barton, Armando Fox

July 2001 **Proceedings of the 7th annual international conference on Mobile computing and networking**

Publisher: ACM Press

Full text available: pdf(691.57 KB) Additional Information: full citation, abstract, references, citings, index terms

Digital appliances designed to simplify everyday tasks are readily available to end consumers.

For example, mobile users can retrieve Web content using handheld devices since content retrieval is well-supported by infrastructure services such as transformational proxies. However, the same type of support is lacking for input-centric devices, those that create content and allow users to share content. This lack of infrastructural support makes input-centric devices hard to use and less useful. ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Results for "(((((((password<in>metadata))<and>(authentication<in>metadata)))<and>(user a..." e-mail
Your search matched **4** of **20** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» Search Options

View Session History

New Search

Modify Search

(((((((password<in>metadata))<and>(authentication<in>metadata)))<and>(user and c Search

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

view selected items Select All Deselect All

1. **Proposal of secure remote access using encryption**
   Kawase, T.; Watanabe, A.; Sasase, I.;
   Global Telecommunications Conference, 1998. GLOBECOM 98. The Bridge to Integration. IEEE
   Volume 2, 8-12 Nov. 1998 Page(s):868 - 873 vol.2
   Digital Object Identifier 10.1109/GLOCOM.1998.776856
   AbstractPlus | Full Text: PDF(340 KB) IEEE CNF
   Rights and Permissions

2. **Parasitic authentication to protect your e-wallet**
   Ebringer, T.; Thorne, P.; Zheng, Y.;
   Computer
   Volume 33, Issue 10, Oct. 2000 Page(s):54 - 60
   Digital Object Identifier 10.1109/2.876293
   AbstractPlus | References | Full Text: PDF(404 KB) IEEE JNL
   Rights and Permissions

3. **New authentication method for mobile centric communications**
   Hongyuan Chen; Sivakumar, T.V.L.N.;
   Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st
   Volume 5, 30 May-1 June 2005 Page(s):2780 - 2784 Vol. 5
   Digital Object Identifier 10.1109/VETECS.2005.1543853
   AbstractPlus | Full Text: PDF(1256 KB) IEEE CNF
   Rights and Permissions

4. **The N/R one time password system**
   Goyal, V.; Abraham, A.; Sanyal, S.; Sang Yong Han;
   Information Technology: Coding and Computing, 2005. ITCC 2005. Internation
   Volume 1, 4-6 April 2005 Page(s):733 - 738 Vol. 1
   Digital Object Identifier 10.1109/ITCC.2005.275
   AbstractPlus | Full Text: PDF(128 KB) IEEE CNF
   Rights and Permissions